Chapitre 1

Eléments de logique et méthodes de démonstration

1.1 Eléments de logique

1.1.1 Assertions

Définition 1.1.1. Une assertion p (ou proposition) est une phrase déclarative exclusivement vraie ou fausse.

Notation 1.1.2. Une table de vérité associe à l'assertion p les deux possibilités : vrai (V) ou faux (F) :

p
V
F

Exemples 1.1.3. *On considère les phrases suivantes :*

1. *Rabat est la capitale du Maroc.*
2. *1+1=3.*
3. *Quelle heure est-il ?*
4. *x+y=z.*

1) est une assertion vraie et 2) est une assertion fausse. 3) et 4) ne sont pas des assertions.

1.1.2 Connecteurs logiques élémentaires

A partir d'assertions $p, q, r, \ldots$, on peut former des assertions à l'aide des **connecteurs logiques** élémentaires suivants :

Définitions 1.1.4. Soit p et q deux assertions.

- La **négation** de p, notée $\neg p$ (ou non p), est l'assertion définie par la table de vérité suivante :

p	$\neg p$
V	F
F	V

- Les connecteurs **et** (**conjonction**) et **ou** (**disjonction**) sont définis par les tables de vérité suivantes :

p	q	p et q	p ou q
V	V	V	V
V	F	F	V
F	V	F	V
F	F	F	F

Notation 1.1.5. L'assertion p et q (resp. p ou q) est notée aussi $p \wedge q$ (resp. $p \vee q$).

Exemples 1.1.6.

1. *Soit p l'assertion "Au moins 100 étudiants assistent au cours d'Algèbre". La négation de p est l'assertion $\neg p$: "Au plus 99 étudiants assistent au cours d'Algèbre".*
2. *On considère l'assertion p : "Aujourd'hui c'est jeudi" et l'assertion q : "Il pleut aujourd'hui". $p \wedge q$ est l'assertion : "Aujourd'hui est jeudi et il pleut aujourd'hui" tandis que l'assertion $p \vee q$ est "Aujourd'hui est jeudi ou il pleut aujourd'hui".*

Remarque 1.1.7. *Soit p et q deux assertions. Le connecteur "ou exclusif" est le connecteur, noté $p \oplus q$, défini par la table de vérité suivante :*

p	q	$p \oplus q$
V	V	F
V	F	V
F	V	V
F	F	F

1.1.3 Implication et équivalence

Définition 1.1.8. Soit p et q deux assertions. On appelle **implication** de q par p l'assertion $(\neg p) \vee q$. L'implication de q par p est notée $p \Rightarrow q$ et se lit "p implique q".

Remarques 1.1.9.

- *L'implication $p \Rightarrow q$ n'est fausse que si p est vraie et q est fausse. Sa table de vérité est la table suivante :*

p	q	$p \Rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

- *L'implication $p \Rightarrow q$ se lit aussi : "si p, alors q" ou "p est une condition suffisante pour avoir q" . On dit aussi que p est l'hypothèse et que q est la conclusion.*
- *L'implication $q \Rightarrow p$ est appelée la réciproque de l'implication $p \Rightarrow q$.*
- *L'implication $\neg q \Rightarrow \neg p$ est appelée la contraposée de l'implication $p \Rightarrow q$.*

Exemple 1.1.10. *On considère les deux propositions suivantes : p : "ABC est un triangle équilatéral", q : "ABC est un triangle isocèle". l'assertion : $p \Rightarrow q$, i.e., "Si ABC est un triangle équilatéral, alors ABC est un triangle isocèle" est une assertion vraie.*

Définition 1.1.11. Soit p et q deux assertions. On appelle **équivalence** de p et q l'assertion $(p \Rightarrow q) \wedge (q \Rightarrow p)$. Cette assertion est notée $p \Leftrightarrow q$ et se lit p **est équivalent à** q.

Remarques 1.1.12.

1. *L'équivalence $p \Leftrightarrow q$ n'est fausse que si l'une des assertions p, q est vraie et l'autre est fausse. Sa table de vérité est la table suivante :*

p	q	$p \Leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

2. *L'équivalence $p \Leftrightarrow q$ se lit aussi : " p est vraie si, et seulement si, q est vraie" ou "pour avoir p, il faut et il suffit d'avoir q" ou "p est une condition nécessaire et suffisante pour avoir q"*
3. *Une **assertion composée** est une assertion formée par une combinaison de plusieurs assertions en utilisant des connecteurs logiques.*

Exemple 1.1.13. *En considérant les assertions p, q de l'exemple précédent, l'assertion : $p \Leftrightarrow q$, i.e., " ABC est un triangle équilatéral si et seulement si ABC est un triangle isocèle" est une assertion fausse.*

Définitions 1.1.14.
- Une **tautologie** est une assertion composée qui est toujours vraie quelles que soient les valeurs de vérité des assertions qui la composent.
- Une **contradiction** est une assertion composée qui est toujours fausse quelles que soient les valeurs de vérité des assertions qui la composent.

Exemples 1.1.15. *Soit p une assertion.*

1. $p \vee (\neg p)$ *est une tautologie.*
2. $p \wedge (\neg p)$ *est une contradiction.*

En mathématique, les résultats portent les noms suivants :
- **théorèmes** : sont les résultats fondamentaux,
- **Propositions** : sont des résulats moins fondamentaux que les théorèmes.
- **Lemmes** : sont les résultats préliminaires.
- **Corollaires** : sont des déductions des résultats précédents.

Proposition 1.1.16. *Soit p, q et r des assertions. Les assertions suivantes sont des tautologies :*

1. $(p \wedge p) \Leftrightarrow p$.
2. $(p \vee p) \Leftrightarrow p$.
3. $(p \wedge q) \Leftrightarrow (q \wedge p)$ *(Commutativité de **et**).*
4. $(p \vee q) \Leftrightarrow (q \vee p)$ *(Commutativité de **ou**).*
5. $[(p \wedge q) \wedge r] \Leftrightarrow [p \wedge (q \wedge r)]$ *(associativité de **et**).*
6. $[(p \vee q) \vee r] \Leftrightarrow [p \vee (q \vee r)]$ *(associativité de **ou**).*
7. $[p \wedge (q \vee r)] \Leftrightarrow [(p \wedge q) \vee (p \wedge r)]$ *(distributivité de **et** par rapport à **ou**).*
8. $[p \vee (q \wedge r)] \Leftrightarrow [(p \vee q) \wedge (p \vee r)]$ *(distributivité de **ou** par rapport à **et**).*
9. $[\neg(\neg p)] \Leftrightarrow p$.
10. $[\neg(p \wedge q)] \Leftrightarrow [(\neg p) \vee (\neg q)]$.
11. $[\neg(p \vee q)] \Leftrightarrow [(\neg p) \wedge (\neg q)]$.
12. $(p \Rightarrow q) \Leftrightarrow [(\neg q) \Rightarrow (\neg p)]$ *(principe de la contraposition).*
13. $[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$ *(transitivité de l'implication).*
14. $[(p \Rightarrow q) \wedge (q \Rightarrow r) \wedge (r \Rightarrow p)] \Leftrightarrow [(p \Leftrightarrow q) \wedge (q \Leftrightarrow r) \wedge (p \Leftrightarrow r)]$.
15. $[p \wedge (p \Rightarrow q)] \Rightarrow q$ *(principe de la déduction).*

Remarque 1.1.17. *Au lieu de dire qu'une assertion p est vraie, on dit : "on a p". Aussi, au lieu de dire que $p \Leftrightarrow q$ est une tautologie, on dit simplement que "les assertions p et q sont équivalentes".*

Exercice 1.1.18. Soit p et q deux assertions.

1. Construire la table de vérité de l'assertion $(p \Rightarrow q) \Leftrightarrow [(\neg p) \vee q]$.
2. En utilisant les propriétés citées dans la proposition précédente, montrer que p et $[(p \vee q) \wedge (\neg((\neg p) \wedge q)]$ sont équivalentes.

1.1.4 Ensembles

Intuitivement, on appelle **ensemble** une collection E d'objets. Ces objets s'appellent les **éléments** de l'ensemble E. Généralement, on note les ensembles avec des lettres majuscules (par exemple, $E, F, \dots$) et les éléments avec des lettres minuscules (par exemple, $x, y, \dots$).

Soit x, y deux éléments d'un ensemble E.
$x = y$ exprime que x et y représente le même objet ou élément de E.
$x \neq y$ signifie $[\neg(x = y)]$.
$x \in E$ exprime que x est un élément de E.
$x \notin E$ signifie que $[\neg(x \in E)]$.
Un ensemble est dit **vide** s'il n'a aucun élément. On note $\emptyset$ l'ensemble vide.
Un ensemble qui n'a qu'un seul élément x est noté $\{x\}$ et appelé **singleton**.

1.1.5 Quantificateurs et prédicats

En mathématiques, on utilise, souvent, des expressions de la forme : "pour tout ...", "quelque soit ...", "il existe au moins ...", "il existe un, et un seul ...", ... Ces expressions précisent comment les éléments d'un ensemble peuvent vérifier une certaine propriété. Ces expressions sont appelées des quantificateurs.
On distingue deux types de quantificateurs :

- Le quantificateur universel, noté $\forall$, se lit "quel que soit", "pour tout",....
- Le quantificateur existentiel, noté $\exists$, se lit "il existe". La notation $\exists!$ signifie "il existe un, et un seul".

Exemple 1.1.19. *Soit $E = \{n \in \mathbb{N}/n > 2\}$. L'assertion : "Pour tout x élément de E, x est supérieur strictement à 2" peut être représentée par :*

$$\forall x \in E, x > 2 \text{ ou par}$$
$$\forall x \in E, P(x), \text{ avec } P(x) \text{ est l'expression "}x \text{ est supérieur strictement à 2".}$$

L'assertion : $\forall x \in E, x > 2$ est une assertion vraie ; cependant, l'assertion : $\exists x \in E : x \leq 2$ est une assertion fausse.

Dans l'exemple précédent, l'expression "$x > 2$" est formée de deux parties : x qui est le sujet et la deuxième partie est "> 2, i.e., la propriété que le sujet x peut vérifié ; cette expression est appelée un **prédicat**.

Exemples 1.1.20.

1. *Soit $P(x)$ l'expression $x > 4$. $P(5)$ est l'assertion $5 > 4$ qui est vraie tandis que $P(3)$ est l'assertion fausse : $3 > 4$.*
2. *Soit $P(x,,y,z)$ l'expression $z = x + y$, alors $P(1,3,4)$ est l'assertion : $4 = 1 + 3$.*

Remarque 1.1.21. *$P(x)$ n'est pas une assertion ; cependant, en attribuant une valeur à x, on obtient une assertion.*

Proposition 1.1.22. *Soit E un ensemble, P et Q des prédicats. Alors, on a les équivalences suivantes :*

1. $[\neg(\forall x \in E, P(x))] \Leftrightarrow \exists x \in E, \neg(P(x))$.
2. $[\neg(\exists x \in E, P(x))] \Leftrightarrow \forall x \in E, \neg(P(x))$.
3. $[\forall x \in E, (P(X) \wedge Q(x)] \Leftrightarrow [(\forall x \in E, P(x)) \wedge (\forall x \in E, Q(x))]$.
4. $[\exists x \in E, (P(X) \vee Q(x))] \Leftrightarrow [(\exists x \in E, P(x)) \vee (\exists x \in E, Q(x))]$.

Exemple 1.1.23. *Soit $(u_n)_{n\in\mathbb{N}}$ une suite réelle.*

- (u_n) *est convergente* $\Leftrightarrow (\exists l \in \mathbb{R})$ *tel que* $(\forall \epsilon > 0), (\exists N \in \mathbb{N}) : (\forall n \in \mathbb{N})$
$$n \geq N \Rightarrow |u_n - l| \leq \epsilon.$$
- (u_n) *est divergente* $\Leftrightarrow (\forall l \in \mathbb{R}), (\exists \epsilon > 0) : (\forall N \in \mathbb{N})(\exists n \in \mathbb{N})$
$$n \geq N \textbf{ et } |u_n - l| > \epsilon.$$

Remarques 1.1.24.

1. *L'ordre des quantificateurs dans une assertion est trés important. Par exemple, l'assertion : $\forall x \in \mathbb{R}^\star, \exists y \in \mathbb{R}^\star : xy = 1$ est vraie tandis que l'assertion : $\exists y \in \mathbb{R}^\star : \forall x \in \mathbb{R}^\star, xy = 1$ est fausse.*
2. *Dans un prédicat $P(x)$, la lettre x est une variable muette ; on peut la remplacer par n'importe quelle autre lettre à condition qu'elle ne soit pas utilisée, auparavant, pour désigner un autre objet.*

Exercice 1.1.25. Soit E l'ensemble des étudiants de la faculté des sciences de Rabat, $P(x)$ (resp. $Q(x)$) l'expression "x parle l'anglais" (resp. "x suit un cours de programmation"). En utilisant les connecteurs logiques et quantificateurs, écrire les expressions suivantes :

1. Il existe un étudiant de la faculté des sciences de Rabat qui parle l'anglais et suit un cours de programmation.
2. Il existe un étudiant de la faculté des sciences de Rabat qui parle l'anglais et qui ne suit aucun cours de programmation.
3. Chaque étudiant de la faculté des sciences de Rabat parle l'anglais ou suit au moins un cours de programmation.

1.2 Méthodes de démonstration

Le long de cette section, p, q et r sont des assertions quelconques.

1.2.1 Démonstration directe

Une démonstration directe de $p \Rightarrow q$ consiste à supposer que p est vraie et étuliser la transitivité de l'implication pour prouver que q est vraie, i.e., en supposant que p est vraie et si les implications $p \Rightarrow r_1, r_1 \Rightarrow r_2, \ldots, r_n \Rightarrow q$ sont vraies, où $r_1, \ldots, r_n$ sont des assertions, alors q est vraie.

Exemple 1.2.1. *Montrons que si m et n sont des entiers impairs, alors mn est un entier impair : supposons que n et m sont des entiers impairs, alors il existe $k, h \in \mathbb{Z}$ tels que $m = 2h+1$ et $n = 2k+1$ d'où $mn = (2h+1)(2k+1) = 2(2hk+h+k)+1$ et ainsi mn est un entier impair.*

1.2.2 Démonstration par disjonction de cas

Pour montrer que r est vraie, il suffit de montrer que :
$p \vee q$ est vraie et que les implications $p \Rightarrow r$ et $q \Rightarrow r$ sont vraies.

Exemple 1.2.2. *Soit $n \in \mathbb{N}$. Montrons que $\frac{n(n+1)}{2} \in \mathbb{N}$: puisque $n \in \mathbb{N}$, alors n est pair ou n est impair, ainsi on distingue les deux cas suivants :*

- *Si n est pair, alors $\frac{n}{2} \in \mathbb{N}$ et ainsi $\frac{n(n+1)}{2} = \frac{n}{2}(n+1) \in \mathbb{N}$.*
- *Si n est impair, alors $n+1$ est pair d'où $\frac{n+1}{2} \in \mathbb{N}$ et ainsi $\frac{n(n+1)}{2} = n\frac{n+1}{2} \in \mathbb{N}$.*

1.2.3 Démonstration par contraposition

Puisque l'implication $p \Rightarrow q$ est équivalente à $\neg q \Rightarrow \neg p$, une démonstration par contraposition de $p \Rightarrow q$ consiste à donner une démonstration directe de $\neg q \Rightarrow \neg p$.

Exemple 1.2.3. *Soit $m, n \in \mathbb{N}$. Montrons que si $a = mn$, alors $m \leq \sqrt{a}$ ou $n \leq \sqrt{a}$: supposons que $m > \sqrt{a}$ et $n > \sqrt{a}$, alors $mn > \sqrt{a}\sqrt{a} = a$ et ainsi $a \neq mn$.*

1.2.4 Démonstration par contre-exemple

Si l'assertion est : "tout élément d'un ensemble E vérifie la proriété P", **l'existence d'un seul élément de E qui ne vérifie pas P montre que l'assertion est fausse**.

Exemple 1.2.4. *Soit $E = \{n \in \mathbb{N}/n > 1\}$. L'assertion : "$\forall n \in E, n-1 \in E$" est fausse car il existe $k = 2 \in E$ tel que $k - 1 = 1 \notin E$.*

Exercice 1.2.5.

1. Donner un contre-exemple pour montrer que les assertions $[(\forall x \in E, P(x)) \vee (\forall x \in E, Q(x))]$ et $[\forall x \in E, (P(x) \vee Q(x)]$ ne sont pas équivalentes.
2. Donner un contre-exemple pour montrer que les assertions $[(\exists x \in E, P(x)) \wedge (\exists x \in E, Q(x))]$ et $[\exists x \in E, (P(x) \wedge Q(x)]$ ne sont pas équivalentes.

1.2.5 Démonstration par l'absurde

Pour montrer, par l'absurde, qu'une assertion p est vraie, on suppose que $\neg p$ est vraie et on montre qu'on obtient alors une contradiction. Ainsi, pour montrer, par l'absurde, l'implication $q \Rightarrow r$, on suppose que r est fausse et que q est vraie (i.e., $q \Rightarrow r$ est fausse) et on montre que l'on aboutit à une contradiction.

Exemples 1.2.6.

1. *Montrons que $\sqrt{2}$ est irrationnel : supposons que $\sqrt{2}$ est rationnel, alors il existe $m \in \mathbb{N}, n \in \mathbb{N}^\star$: $\sqrt{2} = \frac{m}{n}$, avec m et n sans facteur commun (i.e., $\frac{m}{n}$ est irréductible) d'où $2n^2 = m^2$ ainsi m^2 est pair et par suite m est pair d'où il existe $k \in \mathbb{N} : m = 2k$, alors $2n^2 = 4k^2$ ainsi n^2 est pair d'où n est aussi pair et ainsi 2 est un facteur commun de m et n, contradiction.*
2. *Soit n un entier naturel. Montrons par l'absurde que si $3n + 2$ est impair, alors n est impair : supposons alors que n est pair et que $3n + 2$ est impair ; puisque n est pair, $3n + 2$ est pair et on obtient ainsi que $3n + 2$ est pair et $3n + 2$ est impair, contradiction.*

1.2.6 Démonstration par analyse et synthèse

Ce raisonnement est utilisé lors de la recherche des solutions d'un problème. Il est composé de deux étapes :

1. Etape d'analyse : consiste à supposer que le problème est résolu et on cherche les conditions nécessaires.
2. Etape de synthèse : on suppose que ces conditions trouvées dans l'étape d'analyse sont satisfaites et on vérifie qu'elles sont suffisantes.

Exemple 1.2.7. *Soit f une fonction de $\mathbb{R}$ dans $\mathbb{R}$. Montrons que f est la somme d'une fonction paire et d'une fonction impaire :*

1. *Etape d'analyse : On suppose qu'il existe une fonction g de $\mathbb{R}$ dans $\mathbb{R}$ paire et une fonction h de $\mathbb{R}$ dans $\mathbb{R}$ impaire telles que $f = g + h$, alors $\forall x \in \mathbb{R}, f(x) = g(x) + h(x)$ d'où $\forall x \in \mathbb{R}, f(-x) = g(-x) + h(-x)$ et comme g est paire et h est impaire, $\forall x \in \mathbb{R}, f(-x) = g(x) - h(x)$ ainsi $\forall x \in \mathbb{R}, g(x) = \frac{f(x)+f(-x)}{2}$ et $h(x) = \frac{f(x)-f(-x)}{2}$.*
2. *Etape de synthèyse : On vérifie facilement que les fonctions g et h définies ci-dessus sont des solutions de nôtre problème, i.e., on vérfie que g est paire, h est impaire et que $f = g + h$.*

On conclut qu'il existe un unique couple (g, h) tel que $f = g + h$, avec g paire et h impaire.

Chapitre 2

Ensembles, applications et relations binaires

On rappelle qu'un **ensemble** est, intuitivement, une collection E d'objets. Ces objets s'appellent les **éléments** de l'ensemble E.

Le long de ce chapitre, E, F, G et H désignent des ensembles quelconques.

2.1 Opérations sur les ensembles

2.1.1 Parties d'un ensemble

Définition 2.1.1. On dit que F est inclus dans E ou que F est une partie de E si tout élément de F est élément de E. On dira aussi que F est contenu dans E ou que F est un sous-ensemble de E. On écrit $F \subset E$ ou encore $E \supset F$.

Notation 2.1.2. l'ensemble des parties de E est noté $\mathscr{P}(E)$, i.e., $\mathscr{P}(E) = \{A/A \subset E\}$.

Remarques 2.1.3.
- *$A \in \mathscr{P}(E)$ si, et seulement si, $A \subset E$ si, et seulement si, $\forall x \in A, x \in E$.*
- *On a $\emptyset \subset E$ et $E \subset E$.*
- *Si A, B et C sont des parties de E, alors :*
  - *$A \subset B \Leftrightarrow \forall x \in E, (x \in A \Rightarrow x \in B)$.*
  - *$A \not\subset B \Leftrightarrow \exists x \in E : (x \in A$ et $x \notin B)$.*
  - *$A = B \Leftrightarrow A \subset B$ et $B \subset A$.*
  - *$A \subset B$ et $B \subset C \Rightarrow A \subset C$.*

Exemple 2.1.4. *Soit $E = \{a, b\}$. Alors, $\mathscr{P}(E) = \{\emptyset, \{a\}, \{b\}, E\}$.*

Définitions 2.1.5.
- **L'intersection** de E et F, notée $E \cap F$, est l'ensemble défini par $E \cap F := \{x/x \in E$ **et** $x \in F\}$.
- La **réunion** de E et F, notée $E \cup F$, est l'ensemble défini par $E \cup F := \{x/x \in E$ **ou** $x \in F\}$.
- **La différence** de E et F, notée $E \setminus F$, est l'ensemble défini par $E \setminus F := \{x/x \in E$ **et** $x \notin F\}$.
- Si $F \subset E$, l'ensemble $E \setminus F$ est appelé **complémentaire** de F dans E et est noté $\complement_E^F$. Lorsqu'il n'y a aucun risque de confusion, on le note aussi $\overline{F}$.

Remarques 2.1.6.
- *Si $E \cap F = \emptyset$, on dit que E et F sont **disjoints**.*
- *Le complémentaire de F dans E n'est défini que lorsque F est une partie de E.*
- *Si A et B sont deux parties de E, alors $A \setminus B = A \cap \overline{B}$, où $\overline{B} = \complement_E^B$.*

Exemple 2.1.7. *Soit $E = \{x \in \mathbb{R}/|x| \leq 1\}$ et $F = \{x \in \mathbb{R}/|x + 1| \leq 1\}$. Alors, $E \cap F = [-1, 0]$, $E \cup F = [-2, 1]$ et $E \setminus F =]0, 1]$.*

Propriétés 2.1.8. *on a :*
- $E \cap F \subset E$ *et* $E \cap F \subset F$.
- $E \subset E \cup F$ *et* $F \subset E \cup F$.
- $E \cap F = F \cap E$ *(commutativité de l'intersection).*
- $E \cup F = F \cup E$ *(commutativité de la réunion).*
- $E \cap (F \cap G) = (E \cap F) \cap G$ *(associativité de l'intersection).*
- $E \cup (F \cup G) = (E \cup F) \cup G$ *(associativité de la réunion).*
- $E \cap \emptyset = \emptyset$ *(l'ensemble vide est absorbant pour l'intersection).*
- $E \cup \emptyset = E$ *(l'ensemble vide est neutre pour la réunion).*
- $E \cap E = E$ *et* $E \cup E = E$.
- $A \subset E$ *si, et seulement si,* $A \cap E = A$ *si, et seulement si,* $A \cup E = E$.
- $E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$ *(l'intersection est distributive par rapport à la réunion).*
- $E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$ *(la réunion est distributive par rapport à l'intersection).*

Proposition 2.1.9. *Si A et B sont deux parties de E, alors :*
- $\overline{E} = \emptyset$ *et* $\overline{\emptyset} = E$.
- $\overline{\overline{A}} = A$.
- $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
- $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Exercice 2.1.10. Soit A et B deux parties de E. On appelle **différence symétrique** de A et B la partie de E notée $A \triangle B$ et définie par $A \triangle B = (A \setminus B) \cup (B \setminus A)$. Vérifier que

1. $A \triangle B = B \triangle A$.
2. $A \triangle \emptyset = A$.
3. $A \triangle A = \emptyset$.
4. $A \triangle B = (A \cup B) \setminus (A \cap B)$.

2.1.2 Produit cartésien

Définition 2.1.11.
- Le **produit cartésien** de deux ensembles E et F est l'ensemble noté $E \times F := \{(x, y)/x \in E$ et $y \in F\}$. Un élément (x, y) de $E \times F$ est appelé **le couple** (x, y).
- Plus généralemet, si $E_1, \ldots, E_n$ sont n ensembles, $E_1 \times E_2 \times \cdots \times E_n = \{(x_1, \ldots, x_n)/\forall i \in \{1, \ldots, n\}, x_i \in E_i\}$. L'ensemble $E_1 \times E_2 \times \cdots \times E_n$ est noté aussi $\prod_{i=1}^{n} E_i$ et $(x_1, \ldots, x_n)$ est appeleé **n-uplet** de $E_1 \times E_2 \times \cdots \times E_n$.
  Si $E_1 = \cdots = E_n$, on note $E_1 \times E_2 \times \cdots \times E_n = E \times E \times \cdots \times E = E^n$.

Exemple 2.1.12. *On considère les deux ensembles suivants :* $E = \{a, b\}$ *et* $F = \{1, 2\}$, *alors* $E \times F = \{(a, 1), (a, 2), (b, 1), (b, 2)\}$ *et* $E^2 = \{(a, a), (a, b), (b, a), (b, b)\}$.

2.2 Applications

2.2.1 Définitions

Définition 2.2.1. On appelle **correspondance** (ou **relation**) de E vers F tout triplet $f = (E, F, \Gamma)$, où Γ est une partie de $E \times F$.
Si (x, y) est un élément de Γ, y est appeleé **une image** de x par f et x est dit **un antécédent** de y par f. On dit aussi que x est en relation avec y.
Γ est appelé le **graphe de** f.

Notation 2.2.2.
- si $f = (E, F, \Gamma)$ est une correspondance, on écrit $x\ f\ y$ si $(x, y) \in \Gamma$.
- Aussi, une correspondance $f = (E, F, \Gamma)$ est notée :

$$\begin{array}{rccc} f: & E & \to & F \\ & x & \mapsto & f(x) \end{array}$$

où $f(x)$ est un élément de F tel que $(x, f(x)) \in \Gamma$. La correspondance f est notée aussi $E \xrightarrow{f} F$.

Exemple 2.2.3. *Soit $f : \mathbb{R} \to \mathbb{R}, x \mapsto y$, avec y est un réel tel que $y^2 = x$. On remarque que 0 possède une unique image et que si $x \in \mathbb{R}^{\star+}$, x possède deux images distinctes. Cependant, si $x \in \mathbb{R}^{\star-}$, x n'a pas d'image.*

Définition 2.2.4. Soit $f : E \to F$ une correspondance. On dit que f est une **application** de E vers F si pour tout $x \in E$, x possède une, et une seule, image par f, i.e., $\forall x \in E, \exists! y \in F : y = f(x)$.
Si $y = f(x)$, y est dit **l'image** de x par f et on dit aussi que x est un antécédent de y.

Exemples 2.2.5.
1. *La correspondance de l'exemple précédent n'est pas une application.*
2. *La correspondance $f : \mathbb{N} \to \mathbb{N}, n \mapsto n - 1$ n'est pas une application.*
3. *La correspondance $f : \mathbb{R}^+ \to \mathbb{R}, x \mapsto \sqrt{x}$ est une application.*
4. *L'application $id_E : E \to E, x \mapsto x$ est appelée **application identique** (ou **identité** de E).*
5. *Soit A une partie de E. L'application $\chi_A : E \to \{0, 1\}, x \mapsto \begin{cases} 1 \text{ si } x \in A \\ 0 \text{ si } x \notin A \end{cases}$ est appelée **application caractéristique** (ou **indicatrice**) de A.*

Remarques 2.2.6.
- *Soit $f : E \to F$ et $g : G \to H$ deux applications. $f = g$ si, et seulement si, $E = G, F = H$ et $\forall x \in E, f(x) = g(x)$.*
- *Soit A une partie de E et $f : E \to F$ une application. L'application notée $f|_A$ et définie par $f|_A : A \to F, x \mapsto f(x)$ est appelée **restriction** de f à A.*
- *Soit G un ensemble contenant E et $f : E \to F$ une application. Toute application $g : G \to F$ telle que pour tout $x \in E, g(x) = f(x)$ est appelée **prolongement** de f à G.*

Notation 2.2.7. L'ensemble des applications de E vers F est noté $\mathcal{A}(E, F) = F^E$.

2.2.2 Composition des applications

Proposition et Définition 2.2.8. Soit $f : E \to F$ et $g : F \to G$ des applications. L'application de E vers G qui à tout élément x de E associe l'élément $g(f(x))$ de G est appelée composée de f et g et est notée $g \circ f$, i.e., $g \circ f$ est l'application $g \circ f : E \to G, x \mapsto g \circ f(x) = g(f(x))$.

Exemple 2.2.9. *Soit $f : \mathbb{R} \to \mathbb{R}^+, x \mapsto x^2 + 1$ et $g : \mathbb{R}^+ \to \mathbb{R}, x \mapsto \sqrt{x}$, alors $g \circ f : \mathbb{R} \to \mathbb{R}, x \mapsto \sqrt{x^2 + 1}$.*

Proposition 2.2.10. *si $f : E \to F$, $g : F \to G$ et $h : G \to H$ sont des applications, alors $h \circ (g \circ f) = (h \circ g) \circ f$ ($\circ$ est associative).*

Remarque 2.2.11. *La composition des applications n'est pas commutative, en effet, soit E est un ensemble contenant deux éléments a et b distincts, $f, g \in E^E$ telles que $f(a) = b, f(b) = a$ et $g(a) = b, g(b) = b$, alors $g \circ f(a) = b$ tandis que $f \circ g(a) = a$.*

Exercice 2.2.12. Soit A et B deux parties de E. Montrer que
1. $A \subset B$ si, et seulement si, $\chi_A \leq \chi_B$.
2. $A = B$ si, et seulement si, $\chi_A = \chi_B$.
3. $\chi_A^2 = \chi_A$.

4. $\chi_{A\cap B} = \chi_A\chi_B$.
5. $\chi_{\overline{A}} = 1 - \chi_A$, où $1 : E \to \{0,1\}, x \mapsto 1$.
6. $\chi_{A\cup B} = \chi_A + \chi_B - \chi_A\chi_B$.
7. $\chi_{A\setminus B} = \chi_A(1 - \chi_B)$.
8. $\chi_{A\triangle B} = |\chi_A - \chi_B|$.

Exercice 2.2.13. Soit E et F deux ensembles finis. Montrer que si $card(E) = n$ et $card(F) = p$, alors $card(F^E) = p^n$.

2.2.3 Familles

Définition 2.2.14. Soit I un ensemble. Une famille d'éléments de E indexée par I est une application $f : I \to E, i \mapsto f(i) = x_i$. Une famille d'éléments de E indexée par I est notée $(x_i)_{i\in I}$.

Exemples 2.2.15.

1. *Une suite $(u_n)_{n\in\mathbb{N}}$ réelle est une famille de nombres réels indexée par $\mathbb{N}$.*
2. *Si $I = \{1,\dots,n\}$, la famille indexée par I est le n-uplet $(x_1,\dots,x_n)$, où $x_i \in E, \forall i \in I$.*

Remarque 2.2.16. *Lorsque I est fini, on dit que $(x_i)_{i\in I}$ est une famille finie.*

Définitions 2.2.17. Soit I un ensemble et $(E_i)_{i\in I}$ une famille de parties de E indexée par I.
- la partie $\bigcup_{i\in I} E_i = \{x \in E/\exists i \in I, x \in E_i\}$ est appelée **réunion de la famille** $(E_i)_{i\in I}$.
- la partie $\bigcap_{i\in I} E_i = \{x \in E/\forall i \in I, x \in E_i\}$ est appelée **intersection de la famille** $(E_i)_{i\in I}$.

Remarque 2.2.18. *Si A est une partie de E et $(E_i)_{i\in I}$ une famille de parties de E indexée par I, on peut vérifier facilement que :*
- $A \cup (\bigcup_{i\in I} E_i) = \bigcup_{i\in I}(A \cup E_i)$.
- $A \cap (\bigcap_{i\in I} E_i) = \bigcap_{i\in I}(A \cap E_i)$.
- $A \cap (\bigcup_{i\in I} E_i) = \bigcup_{i\in I}(A \cap E_i)$.
- $A \cup (\bigcap_{i\in I} E_i) = \bigcap_{i\in I}(A \cup E_i)$.

2.2.4 Partition

Définitions 2.2.19. Soit $(E_i)_{i\in I}$ une famille de parties de E indexée par un ensemble I.
- On dit que $(E_i)_{i\in I}$ est une **partition** de E si elle vérifie les propriétés suivantes :
  - i) $\forall i \in I, E_i \neq \emptyset$.
  - ii) $\forall i, j \in I$, si $i \neq j$, alors $E_i \cap E_j = \emptyset$.
  - iii) $\bigcup_{i\in I} E_i = E$.
- Soit A une partie de E. On dit que $(E_i)_{i\in I}$ est un **recouvrement** de A si A est contenue dans $\bigcup_{i\in I} E_i$, i.e., $\forall x \in A, \exists i \in I : x \in E_i$.

Remarque 2.2.20. *Une partition de E est un recouvrement de E.*

Exemples 2.2.21.

1. *Posons $A_1 = \mathbb{Z}^+$ et $A_2 = \mathbb{Z}^{\star-}$, (A_1, A_2) est une partition de $\mathbb{Z}$.*
2. *Soit E un ensemble non vide. Alors, la famille $(A_x)_{x\in E}$, où $A_x = \{x\}$, est une partition de E.*
3. *La famille $(A_n)_{n\in\mathbb{N}}$, où $A_n = \{0,\dots,n\}$, est un recouvrement de $\mathbb{N}$; mais $(A_n)_{n\in\mathbb{N}}$ n'est pas une partition de $\mathbb{N}$.*

2.2.5 Image directe et image réciproque

Définitions 2.2.22. Soit $f : E \to F$ une application et A une partie de E. L'ensemble des éléments de F admettant un antécédent par f dans A, noté $f(A)$, est appelé **image de A par f**, i.e., $f(A) = \{y \in F / \exists x \in A, f(x) = y\} = \{f(x) / x \in A\}$. En particulier, si $A = E$, $f(E)$, noté aussi Imf, est dit **image de f**.

Exemple 2.2.23. *Soit $f = \sin : \mathbb{R} \to \mathbb{R}, x \mapsto \sin(x)$; alors $Imf = [-1, 1]$ et $f([0, \frac{\pi}{2}]) = [0, 1]$.*

Propriétés 2.2.24. *Soit A, B deux parties de E et $f : E \to F$ une application.*
- *$f(\emptyset) = \emptyset$.*
- *Si $A \subset B$, alors $f(A) \subset f(B)$.*
- *$f(A \cup B) = f(A) \cup f(B)$. Plus généralement, si $(E_i)_{i \in I}$ est une famille de parties de E, alors $f(\bigcup\limits_{i \in I} E_i) = \bigcup\limits_{i \in I} f(E_i)$.*
- *$f(A \cap B) \subset f(A) \cap f(B)$. Plus généralement, si $(E_i)_{i \in I}$ est une famille de parties de E, alors $f(\bigcap\limits_{i \in I} E_i) \subset \bigcap\limits_{i \in I} f(E_i)$.*

Définitions 2.2.25. Soit $f : E \to F$ une application et B une partie de F. L'ensemble des antécédents par f des éléments de B, noté $f^{-1}(B)$, est appelé **image réciproque** de B par f, i.e., $f^{-1}(B) = \{x \in E / f(x) \in B\}$.

Exemple 2.2.26. *Soit $f = \mathbb{R} \to \mathbb{R}, x \mapsto x^2$, alors $f^{-1}(\mathbb{R}^{\star -}) = \emptyset$ et $f^{-1}(\{4\}) = \{-2, 2\}$.*

Propriétés 2.2.27. *Soit A, B deux parties de F et $f : E \to F$ une application.*
- *$f^{-1}(\emptyset) = \emptyset$.*
- *$f^{-1}(F) = E$.*
- *Si $A \subset B$, alors $f^{-1}(A) \subset f^{-1}(B)$.*
- *$f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$. Plus généralement, si $(E_i)_{i \in I}$ est une famille de parties de E, alors $f^{-1}(\bigcup\limits_{i \in I} E_i) = \bigcup\limits_{i \in I} f^{-1}(E_i)$.*
- *$f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$. Plus généralement, si $(E_i)_{i \in I}$ est une famille de parties de E, alors $f^{-1}(\bigcap\limits_{i \in I} E_i) = \bigcap\limits_{i \in I} f^{-1}(E_i)$.*

2.2.6 Injections, surjections et bijections

Définitions 2.2.28. Soit $f : E \to F$ une application.
- On dit que f est **surjective** (ou une surjection) si tout élément de F admet un antécédent, i.e., $\forall y \in F, \exists x \in E : f(x) = y$.
- On dit que f est **injective** (ou une injection) si tout élément de F admet au plus un antécédent, i.e., $\forall x, x' \in E$, si $f(x) = f(x')$, alors $x = x'$.
- On dit que f est **bijective** (ou une bijection) si f est à la fois surjective et injective (i.e., f est une surjection et une injection).

Exemple 2.2.29.

1. *L'application $f : \mathbb{R} \to \mathbb{R}, x \mapsto |x|$ n'est ni injective ni surjective tandis que $g : \mathbb{R} \to \mathbb{R}^+, x \mapsto |x|$ est surjective.*
2. *id_E est une bijection.*
3. *Soit A une partie de E. L'application $i : A \to E, x \mapsto x$ est une application injective appelée **injection canonique** de A dans E. Si $A \neq E$, i n'est pas surjective.*

Remarque 2.2.30. *Soit $f : E \to F$ une application. f est surjective si, et seulement si, $Imf = F$.*

Proposition 2.2.31.
- *La composée de deux injections est une injection.*
- *La composée de deux surjections est une surjection.*
- *La composée de deux bijections est une bijection.*

Proposition 2.2.32. *Soit $f : E \to F$ et $g : F \to G$ deux applications.*
- *Si $g \circ f$ est injective, alors f est injective.*
- *Si $g \circ f$ est surjective, alors g est surjective.*

Définition 2.2.33. Soit $f : E \to F$ une bijection. L'application qui, à tout élément y de F, associe son unique antécédent par f est appelée **application réciproque de** f et est notée f^{-1}, i.e., f^{-1} est définie par : $(\forall y \in F, \forall x \in E), x = f^{-1}(y) \Leftrightarrow f(x) = y$.

Proposition 2.2.34. *Si $f : E \to F$ est une bijection, alors $f^{-1} \circ f = id_E$ et $f \circ f^{-1} = id_F$.*

Proposition 2.2.35. *Soit $f : E \to F$ et $g : F \to E$ deux applications. Si $f \circ g = id_F$ et $g \circ f = id_E$, alors f et g sont bijectives, $g = f^{-1}$ et $f = g^{-1}$.*

Corollaire 2.2.36.
- *Si $f : E \to F$ est bijective, alors f^{-1} est bijective et $(f^{-1})^{-1} = f$.*
- *Si $f : E \to F$ et $g : F \to G$ sont deux applications bijectives, alors $g \circ f$ est bijective et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

Exemples 2.2.37.
1. *Soit $a \in \mathbb{R}^\star$ et $b \in \mathbb{R}$. L'application $f : \mathbb{R} \to \mathbb{R}, x \mapsto ax+b$ est bijective et l'application réciproque de f est $f^{-1} : \mathbb{R} \to \mathbb{R}, x \mapsto \frac{x-b}{a}$.*
2. *L'application réciproque de $\ln : \mathbb{R}^{\star +} \to \mathbb{R}, x \mapsto \ln(x)$ est l'application $\exp : \mathbb{R} \to \mathbb{R}^{\star +}, x \mapsto \exp(x)$.*

2.3 Relations binaires

2.3.1 Relations d'équivalence

Définition 2.3.1. Une **relation binaire** $\mathcal{R}$ sur E est une correspondance de E vers E, i.e., $\mathcal{R} = (E, E, \Gamma)$, où Γ est une partie de $E \times E$.

Notation 2.3.2. Soit $\mathcal{R}$ sur E et $x, y \in E$. Pour dire que $(x, y) \in \Gamma$, on écrit $x\mathcal{R}y$ et on dit que x est en relation avec y.

Exemple 2.3.3. *Soit $\mathcal{R}$ définie sur $\mathbb{R}$ par $x\mathcal{R}y$ si $x^2 = y^2$, alors $x\mathcal{R}y$ si, et seulement si, $y = \pm x$.*

Définitions 2.3.4. Soit E un ensemble et $\mathcal{R}$ une relation binaire sur E.
- On dit que la relation $\mathcal{R}$ est réflexive si pour tout $x \in E$, $x\mathcal{R}x$.
- On dit que la relation $\mathcal{R}$ est symétrique si pour tout $x, y \in E$, si $x\mathcal{R}y$, alors $y\mathcal{R}x$.
- On dit que la relation $\mathcal{R}$ est transitive si pour tout $x, y, z \in E$, si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $x\mathcal{R}z$.
- On dit que la relation $\mathcal{R}$ est antisymétrique si pour tout $x, y \in E$, si $x\mathcal{R}y$ et $y\mathcal{R}x$, alors $x = y$.
- On dit que la relation $\mathcal{R}$ est ue relation d'équivalence si $\mathcal{R}$ est réflexive, symétrique et transitive.

.

Exemples 2.3.5. *Sur l'ensemble $\mathbb{Z}$, on considère les relations $\mathcal{R}_1$, $\mathcal{R}_2$, $\mathcal{R}_3$, $\mathcal{R}_4$ et $\mathcal{R}_5$ définies par : $x\mathcal{R}_1y$ si $x \leq y$; $x\mathcal{R}_2y$ si $x = y$; $x\mathcal{R}_3y$ si $x = y + 1$; $x\mathcal{R}_4y$ si $x + y \leq 3$; $x\mathcal{R}_5y$ si $x^2 = y^2$. Alors,*
- *$\mathcal{R}_1$ est réflexive, antisymétrique et transitive, mais non symétrique.*
- *$\mathcal{R}_2$ est une relation déquivalence et $\mathcal{R}_2$ est antisymétrique .*
- *$\mathcal{R}_3$ n'est ni réflexive, ni symétrique, et $\mathcal{R}_3$ est antisymétrique.*
- *$\mathcal{R}_4$ n'est ni réflexive, ni antisymétrique, ni transitive et $\mathcal{R}_4$ est symétrique.*
- *$\mathcal{R}_5$ est une relation d'équivalece et $\mathcal{R}_5$ n'est pas antisymétrique.*

Définitions 2.3.6. Soit $\mathcal{R}$ une relation d'équivalence sur E.

- Soit $a \in E$. On appelle **classe d'équivalence** de a (modulo R) le sous-ensemble de E, noté $Cl(a)$ ou $\overline{a}$, défini par $\overline{a} = \{x \in E / x\mathcal{R}a\}$.
- L'ensemble des classes d'équivalence modulo $\mathcal{R}$, noté $E/\mathcal{R}$, est appelé **ensemble quotient** de E par $\mathcal{R}$ ou simplement ensemble quotient, i.e., $E/\mathcal{R} = \{\overline{a} / a \in E\}$.

Exemple 2.3.7. *Soit $x, y \in \mathbb{R}$ et $\mathcal{R}$ la relation définie sur $\mathbb{R}$ par $x\mathcal{R}y$ si $x^2 = y^2$. $\mathcal{R}$ est une relation d'équivalence et on a : $\overline{x} = \{x, -x\}$ et $\mathbb{R}/\mathcal{R} = \{\overline{x} / x \in \mathbb{R}\} = \{\{x, -x\} / x \in \mathbb{R}\}$.*

Remarque 2.3.8. *Soit $\mathcal{R}$ une relation d'équivalence sur E. L'application $s : E \to E/\mathcal{R}, x \mapsto \overline{x}$ est une surjection appelée la **surjection canonique**.*

Proposition 2.3.9. *Soit $x, y \in E$ et $\mathcal{R}$ une relation d'équivalence sur E. Les propositions suivantes sont équivalentes :*

i). $x\mathcal{R}y$.

ii). $\overline{x} = \overline{y}$.

iii). $\overline{x} \cap \overline{y} \neq \emptyset$.

Exemple 2.3.10. *Soit $n \in \mathbb{N} \setminus \{0, 1\}$, $x, y \in \mathbb{Z}$ et $\mathcal{R}$ la relation définie sur $\mathbb{Z}$ par $x\mathcal{R}y$ si n divise $x - y$. $\mathcal{R}$ est une relation d'équivalence et on a : $\overline{x} = x + n\mathbb{Z}$, où $n\mathbb{Z} = \{nk / k \in \mathbb{Z}\}$ et $\mathbb{Z}/\mathcal{R} = \{\overline{x} / x \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. La relation $\mathcal{R}$ est appelée **congruence modulo n**. Aussi, au lieu décrire $x\mathcal{R}y$, on écrit $x \equiv y \pmod{n}$ et on dit que x est congru à y modulo n. Pour la congruence modulo n, l'ensemble quotient $\mathbb{Z}/\mathcal{R}$ est noté $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}_n$.*

Théorème 2.3.11.

- *Si $\mathcal{R}$ une relation déquivalence sur E, alors la famille $(\overline{x})_{\overline{x} \in E/\mathcal{R}}$ forme une partition de E*
- *Réciproquement, si une famille $(A_i)_{i \in I}$ de parties de E, où I est un ensemble, est une partition de E, alors la relation $\mathcal{R}$ définie sur E par $x\mathcal{R}y$ s'il existe $i \in I : x, y \in A_i$ est une relation d'équivalence sur E.*

Théorème 2.3.12. *(**Décomposition canonique d'une application**) Si $f : E \to F$ est une application, alors :*

- *La relation $\mathcal{R}$ définie sur E par $x\mathcal{R}y$ si $f(x) = f(y)$, où $x, y \in E$, est une relation d'équivalence.*
- *il existe une, et une seule, application $\overline{f} : E/\mathcal{R} \to Imf$ telle que $\overline{f}$ est bijective et $f = i \circ \overline{f} \circ s$, avec $i : Imf \to F$ (resp. $s : E \to E/\mathcal{R}$) est l'injection canonique (resp. la surjection canonique).*

*La décomposition $f = i \circ \overline{f} \circ s$ est appelée **la décomposition canonique de** f.*

Exemple 2.3.13. *Soit $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$. La décomposition canonique de f est $f = i \circ \overline{f} \circ s$, avec s est la surjection canonique $s : \mathbb{R} \to \mathbb{R}/\mathcal{R} = \{\{x, -x\} / x \in \mathbb{R}\}, x \mapsto \overline{x} = \{x, -x\}$, $\overline{f}$ est la bijection $\overline{f} : \mathbb{R}/\mathcal{R} \to \mathbb{R}^+, \{x, -x\} \mapsto x^2$ et i est l'injection canonique $i : \mathbb{R}^+ \to \mathbb{R}, x \mapsto x$.*

2.3.2 Relations d'ordre

Définitions et exemples

Définition 2.3.14. Soit $\mathcal{R}$ une relation binaire sur E. On dit que $\mathcal{R}$ est une **relation d'ordre** (ou un ordre) sur E si $\mathcal{R}$ est réflexive, antisymétrique et transitive.

Notation 2.3.15. Soit $\mathcal{R}$ une relation d'ordre sur E et $x, y \in E$. Si $x\mathcal{R}y$, on note $x \preceq y$ au lieu de $x\mathcal{R}y$.

Remarques 2.3.16.

- *Si $\preceq$ est un ordre sur E, $(E, \preceq)$ est dit **ensemble ordonné**.*
- *Soit $(E, \preceq)$ un ensemble ordonné. L'ordre strict associé à l'ordre $\preceq$ est la relation binaire, notée $\prec$, définie dans E par : $\forall x, y \in E$, $x \prec y$ si ($x \preceq y$ et $x \neq y$).*
- *Une relation binaire dans E qui est réflexive et transitive et dite un **préordre** sur E.*

Exemples 2.3.17.

1. $(\mathbb{N}, \leq), (\mathbb{Z}, \leq), (\mathbb{Q}, \leq), (\mathbb{R}, \leq)$ *sont des ensembles ordonnés avec* $\leq$ *est l'ordre usuel.*
2. $(\mathcal{P}(E), \subset)$ *est un ensemble ordonné.*
3. *Soit* $|$ *la relation définie sur* $\mathbb{N}^\star$ *par :* $m \mid n$ *si* m *divise* n. *Alors* $(\mathbb{N}^\star, |)$ *est un ensemble ordonné.*
4. *Dans* $\mathbb{Z}$, $|$ *n'est pas une relation d'ordre ;* $|$ *est un préordre sur* $\mathbb{Z}$.
5. *Dans* $\mathbb{C}$, *la relation* $\mathcal{R}$ *définie par* $z\mathcal{R}z'$ *si* $|z| \leq |z'|$ *est un préordre.*

Exercice 2.3.18. Soit $\mathcal{R}$ un préordre dans E. On considère la relation $\mathcal{S}$ définie sur E par : $x\mathcal{S}y$ si $x\mathcal{R}y$ et $y\mathcal{R}x$. Montrer que $\mathcal{S}$ est une relation d'équivalence.

Définition 2.3.19. Soit $\preceq$ un ordre dans E.

- On dit que $\preceq$ est un **ordre total** si $\forall x, y \in E$, x et y sont comparables, i.e., $\forall x, y \in E$, $x \preceq y$ ou $y \preceq x$.
- Si l'ordre $\preceq$ n'est pas total, on dit que $\preceq$ est un **ordre partiel**.

Exemples 2.3.20.

1. $(\mathbb{N}, \leq), (\mathbb{Z}, \leq), (\mathbb{Q}, \leq), (\mathbb{R}, \leq)$ *sont des ensembles totalement ordonnés.*
2. *Si* E *contient deux éléments distincts, l'inclusion dans* $\mathcal{P}(E)$ *est un ordre partiel.*
3. $|$ *est un orde partiel dans* $\mathbb{N}^\star$.

Eléments remarquables

Définitions 2.3.21. Soit $(E, \preceq)$ un ensemble ordonné, A une partie de E, M et m deux éléments de E.

- On dit que M est **un majorant** de A dans E si $\forall x \in A, x \preceq M$.
- On dit que m est **un minorant** de A dans E si $\forall x \in A, m \preceq x$.
- On dit que A est **majorée** (resp. **minorée**) dans E si A admet un majorant (resp. minorant) dans E.
- On dit que M est un **plus grand élément** de A si
  i) $M \in A$
  ii) $\forall x \in A, x \preceq M$.
- On dit que m est un **plus petit élément** de A si
  i) $m \in A$
  ii) $\forall x \in A, m \preceq x$.

Remarque 2.3.22. *Soit* $(E, \preceq)$ *un ensemble ordonné. Si* A *est une partie de* E, *alors* A *possède au plus un plus grand élément (resp. un plus petit élément).*

Exemples 2.3.23.

1. *Dans* $(\mathbb{N}^\star, |)$, *la partie* $A = \{2, 4, 5\}$ *est majorée dans* $\mathbb{N}^\star$ *(par exemple,* 20 *est un majorant de* A *dans* $\mathbb{N}^\star$. *Aussi, la partie* $A = \{2, 6, 10\}$ *est minorée dans* $\mathbb{N}^\star$ *(par exemple,* 2 *est un minorant de* A *dans* $\mathbb{N}^\star$.
2. *Dans* $(\mathbb{N}^\star, |)$, 2 *est le plus petit élément de* $A = \{2, 6, 10\}$.
3. *Dans* $(\mathcal{P}(E), \subset)$, *si* $X, Y \in \mathcal{P}(E)$, *la partie* $A = \{X, Y\}$ *est minorée et majorée dans* $\mathcal{P}(E)$ *(*$X \cap Y$ *(resp.* $X \cup Y$*) est un minorant (resp. un majorant) de* A *dans* $\mathcal{P}(E)$*).*
4. *La partie* $A =]0, 1[$ *de* $\mathbb{R}$ *ordonné par l'ordre usuel est une partie majorée et minorée de* $\mathbb{R}$, *mais* A *n'admet ni un plus grand élément ni un plus petit élément.*

Définitions 2.3.24. Soit $(E, \preceq)$ un ensemble ordonné et A une partie de E.

- **La borne supérieure** de A dans E, si elle existe , est l'élément, noté $\sup_E A$ (ou $\sup A$), vérifiant :

i) $\sup A$ est un majorant de A dans E.

ii) Soit $M \in E$. Si M est un majorant de A dans E, alors $\sup A \preceq M$.

– **La borne inférieure** de A dans E, si elle existe, est l'élément, noté $\inf_E A$ (ou $\inf A$) vérifiant :

i) $\inf A$ est un minorant de A dans E.

ii) Soit $m \in E$. Si m est un minorant de A dans E, alors $m \preceq \inf A$.

Remarques 2.3.25. *Soit $(E, \preceq)$ un ensemble ordonné et A une partie de E.*

– $\sup A$ *est le plus petit élément, lorsqu'il existe, de l'ensemble des majorants de A dans E.*

– $\inf A$ *est le plus grand élément, lorsqu'il existe, de l'ensemble des minorants de A dans E.*

Exemples 2.3.26.

1. *Dans $(\mathbb{N}^\star, |)$, on considère $A = \{2, 6, 10\}$, alors $\sup A = 30$ et $\inf A = 2$ (2 est le plus petit élément de A).*
2. *Dans $(\mathcal{P}(E), \subset)$, si $X, Y \in \mathcal{P}(E)$ et $A = \{X, Y\}$, alors $\sup A = X \cup Y$ et $\inf A = X \cap Y$.*

Définitions 2.3.27. Soit $(E, \preceq)$ un ensemble ordonné, A une partie de E, m et M deux éléments de A.

– On dit que M est un **élément maximal** de A si $\forall x \in A, (M \preceq x \Rightarrow x = M)$.

– On dit que M est un **élément minimal** de A si $\forall x \in A, (x \preceq m \Rightarrow x = m)$.

Exemples 2.3.28.

1. *Dans $(\mathbb{N}^\star, |)$, on considère $A = \{2, 3, 4, 5, 6, 7, 8, 9\}$, alors, $5, 6, 7, 8, 9$ sont des éléments maximaux de A et $2, 3, 5$ et 7 sont des éléments minimaux de A.*
2. *Dans $(\mathbb{N}^\star, |)$, on considère $A = \mathbb{N}^\star \setminus \{1\}$, alors les nombres premiers sont des éléments minimaux de A.*

Chapitre 3

Arithmétique dans $\mathbb{Z}$

3.1 Ensemble des entiers naturels

3.1.1 Définitions

On admet l'existence d'un ensemble ordonné non vide $(\mathbb{N}, \leq)$ vérifiant les trois propriétés suivantes :

i) Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.

ii) Toute partie non vide majorée de $\mathbb{N}$ possède un plus grand élément.

iii) $\mathbb{N}$ n'a pas de plus grand élément.

Remarques 3.1.1.
- *L'ensemble* $\mathbb{N}$ *est totalement ordonné.*
- *L'ensemble* $\mathbb{N}$ *n'est pas majoré.*
- 0 *est le plus petit élément de* $\mathbb{N}$. *L'ensemble* $\mathbb{N}$ *privé de* 0 *est noté* $\mathbb{N}^\star$.
- *Si* $n \in \mathbb{N}$, $n+1$ *est appelé successeur de* n.
- *Si* $n \in \mathbb{N}^\star$, $n-1$ *est appelé prédécsseur de* n.

Théorème 3.1.2. ***(Propriété d'archimède)*** $\forall a \in \mathbb{N}$, $\forall b \in \mathbb{N}^\star$, $\exists n \in \mathbb{N} : nb \geq a$.

3.1.2 Raisonnement par récurrence

Théorème 3.1.3. ***(Principe de l'induction mathématique)*** *Soit* $n_0 \in \mathbb{N}$ *et* $P(n)$ *une proposition dépendante de* n, *où* $n \in \mathbb{N}$. *Si*

1. $P(n_0)$ *est vraie,*
2. *Pour tout entier* $n \geq n_0$, *si* $P(n)$ *est vraie, alors* $P(n+1)$ *est vraie,*

alors Pour tout entier $n \geq n_0$, $P(n)$ *est vraie.*

Exercice 3.1.4.

1. Montrer que $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.
2. Montrer que $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

Théorème 3.1.5. ***(Récurrence à deux pas)*** *Soit* $n_0 \in \mathbb{N}$ *et* $P(n)$ *une proposition dépendante de* n, *où* $n \in \mathbb{N}$. *Si*

1. $P(n_0)$ *et* $P(n_0+1)$ *sont vraies,*
2. *Pour tout entier* $n \geq n_0$, $P(n)$ *et* $P(n+1)$ *sont vraies implique* $P(n+2)$ *est vraie,*

alors Pour tout entier $n \geq n_0$, $P(n)$ *est vraie.*

Exercice 3.1.6. Soit (u_n) la suite réelle définie par $u_0 = 2$, $u_1 = 5$ et pour tout entier $n \geq 0$, $u_{n+2} = 5u_{n+1} - 6u_n$. Montrer par récurrence à deux pas que $\forall n \in \mathbb{N}, u_n = 2^n + 3^n$.

Théorème 3.1.7. ***(Récurrence forte)*** *Soit $n_0 \in \mathbb{N}$ et $P(n)$ une proposition dépendante de n, où $n \in \mathbb{N}$. Si*

1. *$P(n_0)$ est vraie,*
2. *Pour tout entier $n \geq n_0$, si pour tout entier k tel que $n_0 \leq k \leq n$, $P(k)$ est vraie implique $P(n+1)$ est vraie,*

alors Pour tout entier $n \geq n_0$, $P(n)$ est vraie.

Exercice 3.1.8. Soit n un entier naturel non nul. Montrer par récurrence forte qu'il existe $k, m \in \mathbb{N}$ tels que $n = 2^k(2m+1)$.

3.2 Divisibilité dans $\mathbb{Z}$

Théorème 3.2.1. ***(Thóerème de la division euclidienne dans $\mathbb{Z}$)*** *$\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}^\star$, $\exists !(q,r) \in \mathbb{Z}^2$ tel que $a = bq + r$, avec $0 \leq r < |b|$.*
q est appelé ***quotient*** *de la division euclidienne de a par b et r est* ***le reste****.*

Théorème 3.2.2. ***(Thóerème de la division euclidienne dans $\mathbb{N}$)*** *$\forall (a,b) \in \mathbb{N} \times \mathbb{N}^\star$, $\exists !(q,r) \in \mathbb{N} \times \mathbb{N}$ tel que $a = bq + r$, avec $0 \leq r < b$.*

Exemples 3.2.3.

1. *Pour $a = 2015$ et $b = 15$, on a $q = [\frac{a}{b}] = 134$ et $r = a - bq = 5$.*
2. *Pour $a = -2016$ et $b = 67$, on a $q = [\frac{a}{b}] = -31$ et $r = a - bq = 61$.*

Définition 3.2.4. Soit $a, b \in \mathbb{Z}$. On dit que a divise b s'il existe $c \in \mathbb{Z}$ tel que $b = ac$. Lorsque a divise b, on écrit $a \mid b$.

Remarque 3.2.5. *Soit $a, b \in \mathbb{Z}$. Si a divise b, on dit que a est un diviseur de b ou b est un multiple de a ou b est divisible par a.*

Propriétés 3.2.6. *Soit a, b, c et d des entiers.*

i) $a \mid 0$ *et si* $0 \mid b$, *alors* $b = 0$.

ii) $a \mid 1$ *si, et seulement si,* $a = \pm 1$.

iii) $a \mid b$ *et* $b \mid a$ *si, et seulement si,* $a = \pm b$.

iv) Si $a \mid b$ *et* $c \mid d$, *alors* $ac \mid bd$.

v) Si $a \mid b$ *et* $b \mid c$, *alors* $a \mid c$.

vi) Si $a \mid b$ *et* $b \neq 0$, *alors* $|a| \leq |b|$.

vii) Si $a \mid b$ *et* $a \mid c$ *; alors pour tout* $(x, y) \in \mathbb{Z}$, $a \mid bx + cy$.

Remarque 3.2.7. *La relation de divisibilité dans $\mathbb{Z}$ est réflexive et transitive mais n'est pas antisymétrique.*

3.3 Pgcd et Ppcm

Théorème et Définition 3.3.1. Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. Il existe un unique entier positif d tel que

i) $d \mid a$ et $d \mid b$,

ii) Si c est un entier tel que c divise a et c divise b, alors $c \leq d$.

L'entier naturel d est appelé **le plus grand commun diviseur** de a et b. d est noté $a \wedge b$ ou $d = pgcd(a, b)$.

Remarque 3.3.2.

1. *Si $(a, b) \in \mathbb{Z}^2 - \{(0, 0)\}$, alors il existe $(x, y) \in \mathbb{Z}^2 : a \wedge b = ax + by$.*
2. *On vérifie que si a, b et c sont des entiers non nuls, alors $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ et ainsi on peut généraliser, par récurrence, à un nombre fini quelconque d'entiers non nuls, i.e., $a_1 \wedge \cdots \wedge a_n = (a_1 \wedge \cdots \wedge a_{n-1}) \wedge a_n$.*

Théorème 3.3.3. *Soit $(a, b) \in \mathbb{Z} - \{(0, 0)\}$ et $d \in \mathbb{N}$. $d = a \wedge b$ si, et seulement si,*

i) $d \mid a$ et $d \mid b$,

ii) Si c est un entier tel que $c \mid a$ et $c \mid b$, alors $c \mid d$.

Définition 3.3.4. Soit $(a, b) \in \mathbb{Z}^2 - \{(0, 0)\}$. On dit que a et b sont premiers entre eux si $a \wedge b = 1$.

Théorème 3.3.5. ***(Théorème de Bézout)*** *Soit $(a, b) \in \mathbb{Z} - \{(0, 0)\}$. a et b sont premiers entre eux si, et seulement si, il existe $x, y \in \mathbb{Z}$ tels que $1 = ax + by$.*

Corollaire 3.3.6. *Soit $(a, b) \in \mathbb{Z} - \{(0, 0)\}$. Si $a \wedge b = d$, alors $\frac{a}{d} \wedge \frac{b}{d} = 1$.*

Corollaire 3.3.7. *Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid c$ et $b \mid c$. Si $a \wedge b = 1$, alors $ab \mid c$.*

Théorème 3.3.8. ***(Lemme de Gauss)*** *Soit $a, b, c \in \mathbb{Z}$ tels que $a \mid bc$. Si $a \wedge b = 1$, alors $a \mid c$.*

3.4 Algorithme d'Euclide

Lemme 3.4.1. *Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^\star$. Si $a = qb + r$, où $q, r \in \mathbb{Z}$, alors $a \wedge b = b \wedge r$.*

Algorithme 3.4.2. ***(Algorithme d'Euclide)****Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^\star$. Puisque $a \wedge b = |a| \wedge |b|$, on peut supposer que $0 < b \leq a$. En effectuant la division euclidienne de a par b, on a $a = q_1 b + r_1$, avec $0 \leq r_1 < b$. Si $r_1 = 0$, alors $a \wedge b = b$. Si $r_1 \neq 0$, on effectue la division euclidienne de b par r_1 et on obtient $b = q_2 r_1 + r_2$, avec $0 \leq r_2 < r_1$. Si $r_2 = 0$, alors $a \wedge b = b \wedge r_1 = r_1$. Si $r_2 \neq 0$, on continue en effectuant la division euclidienne de r_1 par r_2 ; ce processus de division successives continue jusqu'à ce que un reste r_{n+1} nul apparait (l'apparition d'un reste nul est dûe au fait que $b > r_1 > r_2 > \cdots \geq 0$ et $b, r_1, r_2, \cdots \in \mathbb{N}$). On obtient ainsi :*

$$\begin{gathered} a = bq + r_1, \text{ avec } 0 \leq r_1 < b \\ b = q_2 r_1 + r_2, \text{ avec } 0 \leq r_2 < r_1 \\ r_1 = q_3 r_2 + r_3, \text{ avec } 0 \leq r_3 < r_2 \\ \vdots \\ r_{n-2} = q_n r_{n-1} + r_n, \text{ avec } 0 \leq r_n < r_{n-1} \\ r_{n-1} = q_{n+1} r_n \end{gathered}$$

Ainsi, on a $a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = \cdots = r_{n-1} \wedge r_n = r_n$.

Exemple 3.4.3. *En utilisant l'algorithme d'Euclide pour calculer $1008 \wedge 360$, on obtient :* $1008 = 2.360 + 288$, $360 = 288.1 + 72$, $288 = 72.4$ *ainsi* $1008 \wedge 360 = 72$.

Algorithme 3.4.4. ***(Algorithme d'Euclide étendu)*** *Soit a et b deux entiers et $d = a \wedge b$. L'algorithme suivant permet décrire d comme combinaison de a et b, i.e., trouver $x, y \in \mathbb{Z} : d = ax + by$: on part de $d = r_n = r_{n-2} - q_n r_{n-1}$ puis on exprime d comme combinaison de r_{n-2} et r_{n-3} et en remontant des bas en haut, on écrit d comme combinaison de b et r_1 et ainsi on obtient d sous la forme $d = ax + by$.*

Exemple 3.4.5. *On a* $1008 \wedge 360 = 72$ *et* $72 = 360 - 288.1 = 360 - (1008 - 2.360)$ *ainsi* $72 = (-1).1008 + 3.36$.

Corollaire 3.4.6. *Si k est un entier non nul, alors $pgcd(ka, kb) = |k|pgcd(a, b)$.*

Théorème et Définition 3.4.7. Soit $(a, b) \in \mathbb{Z}^2 - \{(0, 0)\}$. Il existe un unique entier positif m tel que

i) $a \mid m$ et $b \mid m$,

ii) Si c est un entier tel que a divise c et b divise c, alors m divise c.

L'entier naturel m est appelé **le plus petit commun multiple** de a et b. m est noté $a \vee b$ ou $m = ppcm(a, b)$.

Remarque 3.4.8. *On vérifie que si a, b et c sont des entiers non nuls, alors $(a \vee b) \vee c = a \vee (b \vee c)$ et ainsi on peut généraliser, par récurrence, à un nombre fini quelconque d'entiers non nuls, i.e., $a_1 \vee \cdots \vee a_n = (a_1 \vee \cdots \vee a_{n-1}) \vee a_n$.*

Théorème 3.4.9. *Soit $a, b, c \in \mathbb{Z} - \{0\}$. Alors, $pgcd(a, b)ppcm(a, b) = |ab|$.*

Exercice 3.4.10. Soit $a, b, c \in \mathbb{Z} - \{0\}$. Alors $ab \vee ac = |a|(b \vee c)$.

3.5 Nombres premiers

Définition 3.5.1. Soit $p > 1$ un entier. On dit que p est **premier** si les seuls diviseurs positifs de p sont 1 et p. Un entier > 1 qui n'est pas premier est dit **composé**.

Théorème 3.5.2. *Soit $a, b \in \mathbb{Z}$ et p un nombre premier. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.*

Corollaire 3.5.3. *Soit p un nombre premier.*

1. *Soit $a_1, \ldots, a_n \in \mathbb{Z}$. Si $p \mid a_1 \ldots a_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p \mid a_k$.*
2. *Soit $p_1, \ldots, p_n$ des nombres premiers. Si $p \mid p_1 \ldots p_n$, alors il existe $k \in \{1, \ldots, n\}$ tel que $p = p_k$.*

Théorème 3.5.4. ***(Théorème fondamental d'arithmétique)*** *Si $n > 1$ est un entier, alors n s'écrit d'une manière unique sous la forme $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, avec pour tout $i = 1, \ldots, r$, $k_i \in \mathbb{N}^\star$, p_i est premier et $p_1 < p_2 < \cdots < p_r$.*

Théorème 3.5.5. ***(Théorème d'Euclide)*** *Il existe une infinité de nombres premiers.*

Exercice 3.5.6. Montrer que si $n > 1$ est un entier composé, alors n possède un diviseur premier p tel que $p \leq \sqrt{n}$.

3.6 Congruences

Définition 3.6.1. Soit $n \in \mathbb{N}$. On dit que deux entiers relatifs a et b sont congrus modulo n et on note $a \equiv b \ (\mod n)$ si n divise $a - b$. La relation $a \equiv b \ (\mod n)$ est appelée **congruence modulo n**.

Remarque 3.6.2. *Si $n = 0$, la relation $a \equiv b \ (\mod n)$ n'est autre que $a = b$. Si $n = 1$, la relation $a \equiv b \ (\mod n)$ est vraie pour tout $(a, b) \in \mathbb{Z}^2$.*
Dans la suite de cette section, on suppose que $n \geq 2$.

Théorème 3.6.3. *Soit $n \geq 2$ un entier. La relation $a \equiv b \ (\mod n)$ définie sur $\mathbb{Z}$ est une relation d'équivalence.*

Remarques 3.6.4.

1. *L'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}_n$.*
2. *Dans chaque classe de congruence modulo n, il existe un, et un seul, entier appartenant à l'ensemble $\{0, 1 \ldots, n-1\}$, i.e., si $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$, $\exists! a \in \overline{x}$ tel que $a \in \{0, 1 \ldots, n-1\}$.*

Théorème 3.6.5. *Soit $n \geq 2$ un entier, a_1, a_2, b_1 et b_2 des entiers relatifs.*

1. *Si $a_1 \equiv b_1$ (mod n) et $a_2 \equiv b_2$ (mod n), alors $a_1 + a_2 \equiv b_1 + b_2$ (mod n) (**Compatibilité de la congruence** mod n **avec l'addition dans** $\mathbb{Z}$)*
2. *Si $a_1 \equiv b_1$ (mod n) et $a_2 \equiv b_2$ (mod n), alors $a_1 a_2 \equiv b_1 b_2$ (mod n) (**Compatibilité de la congruence** mod n **avec la multiplication dans** $\mathbb{Z}$)*

3.7 L'anneau $\mathbb{Z}/n\mathbb{Z}$

On définit dans $\mathbb{Z}/n\mathbb{Z}$ deux lois de composition : une additivement et l'autre multiplicativement :
- **Addition :** Soit $\overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}$, on définit $\overline{x} + \overline{y} := \overline{x + y}$.
- **Multiplication :** Soit $\overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}$, on définit $\overline{x}.\overline{y} := \overline{xy}$.

Théorème 3.7.1. *L'addition et la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ munissent cet ensemble d'une structure d'anneau commutatif non trivial. Cet anneau admet $\overline{0}$ pour élément nul et $\overline{1}$ pour unité.*

Théorème 3.7.2. *La correspondance $f : \{0, 1, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x}$ et une bijection et ainsi $\mathbb{Z}/n\mathbb{Z}$ est un ensemble fini ayant n éléments.*

Théorème 3.7.3. *$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.*

Théorème 3.7.4. ***(Petit théorème de Fermat)** Soit $a \in \mathbb{Z}$ et p un nombre premier. Si p ne divise pas a, alors $a^{p-1} \equiv 1$(mod p).*

Corollaire 3.7.5. *Si p est un nombre premier, alors pour tout $a \in \mathbb{Z}$, $a^p \equiv a$(mod p).*

Exercice 3.7.6. Soit $n > 1$ un entier, $a, b, c \in \mathbb{Z}$.

1. Montrer que si $a \equiv b$ (mod n), alors $a^k \equiv b^k$ (mod n), pour tout entier $k > 0$.
2. On suppose que a, b et c sont non nuls. Montrer que si $ac \equiv bc$ (mod n), alors $a \equiv b$ (mod $\frac{n}{d}$), où $d = c \wedge n$.

3.8 Fonction indicatrice d'Euler

Définition 3.8.1. Pour tout entier $n \geq 1$, on note $\varphi(n)$ le nombre des entiers $k \in \{0, 1, \ldots, n-1\}$ tels que $k \wedge n = 1$, i.e., $\varphi(n) = card\{k \in \{0, 1, \ldots, n-1\}/k \wedge n = 1\}$. L'application φ est appelée la **fonction indicatrice d'Euler** ou **l'indicateur d'Euler** et $\varphi(n)$ est dit indicateur d'Euler de n.

Exemple 3.8.2. *On a $\varphi(1) = 1, \varphi(2) = 1, \varphi(10) = 4$.*

Théorème 3.8.3. *Si p est un nombre premier et $k > 0$ est un entier, alors $\varphi(p^k) = p^k - p^{k-1}$.*

Lemme 3.8.4. *Soit $a, b, c \in \mathbb{N}$. $a \wedge bc = 1$ si, et seulement si, $a \wedge b = 1$ et $a \wedge c = 1$.*

Théorème 3.8.5. *Soit $m, n \in \mathbb{N} - \{0, 1\}$. Si m et n sont premiers entre eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$.*

Théorème 3.8.6. *Soit $n > 1$ un entier et $n = p_1^{k_1} \ldots p_r^{k_r}$, avec $p_1, \ldots, p_r$ des nombres premiers et $k_1, \ldots, k_r$ des entiers > 0, alors $\varphi(n) = (p_1^{k_1} - p_1^{k_1 - 1}) \ldots (p_r^{k_r} - p_r^{k_r - 1}) = n(1 - \frac{1}{p_1}) \ldots (1 - \frac{1}{p_r})$.*

Exemple 3.8.7. *on a $1800 = 2^3 3^2 5^2$, alors $\varphi(1300) = 480$.*